Configuring VINES Services

BayRS Version 13.00
Site Manager Software Version 7.00

Part No. 303544-A Rev 00
October 1998

Bay Networks *Where Information Flows.*™

4401 Great America Parkway
Santa Clara, CA 95054

8 Federal Street
Billerica, MA 01821

Copyright © 1998 Bay Networks, Inc.

All rights reserved. Printed in the USA. October 1998.

The information in this document is subject to change without notice. The statements, configurations, technical data, and recommendations in this document are believed to be accurate and reliable, but are presented without express or implied warranty. Users must take full responsibility for their applications of any products specified in this document. The information in this document is proprietary to Bay Networks, Inc.

The software described in this document is furnished under a license agreement and may only be used in accordance with the terms of that license. A summary of the Software License is included in this document.

Trademarks

AN, BCN, BLN, BN, FRE, Optivity, PPX, and Bay Networks are registered trademarks and Advanced Remote Node, ANH, ARN, ASN, BayRS, BaySecure, BayStack, BayStream, BCC, SPEX, System 5000, and the Bay Networks logo are trademarks of Bay Networks, Inc.

Microsoft, MS, MS-DOS, Win32, Windows, Internet Explorer, and Windows NT are registered trademarks of Microsoft Corporation.

All other trademarks and registered trademarks are the property of their respective owners.

Restricted Rights Legend

Use, duplication, or disclosure by the United States Government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013.

Notwithstanding any other license agreement that may pertain to, or accompany the delivery of, this computer software, the rights of the United States Government regarding its use, reproduction, and disclosure are as set forth in the Commercial Computer Software-Restricted Rights clause at FAR 52.227-19.

Statement of Conditions

In the interest of improving internal design, operational function, and/or reliability, Bay Networks, Inc. reserves the right to make changes to the products described in this document without notice.

Bay Networks, Inc. does not assume any liability that may occur due to the use or application of the product(s) or circuit layout(s) described herein.

Portions of the code in this software product may be Copyright © 1988, Regents of the University of California. All rights reserved. Redistribution and use in source and binary forms of such portions are permitted, provided that the above copyright notice and this paragraph are duplicated in all such forms and that any documentation, advertising materials, and other materials related to such distribution and use acknowledge that such portions of the software were developed by the University of California, Berkeley. The name of the University may not be used to endorse or promote products derived from such portions of the software without specific prior written permission.

SUCH PORTIONS OF THE SOFTWARE ARE PROVIDED “AS IS” AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

In addition, the program and information contained herein are licensed only pursuant to a license agreement that contains restrictions on use and disclosure (that may incorporate by reference certain limitations and notices imposed by third parties).

Bay Networks, Inc. Software License Agreement

NOTICE: Please carefully read this license agreement before copying or using the accompanying software or installing the hardware unit with pre-enabled software (each of which is referred to as "Software" in this Agreement). BY COPYING OR USING THE SOFTWARE, YOU ACCEPT ALL OF THE TERMS AND CONDITIONS OF THIS LICENSE AGREEMENT. THE TERMS EXPRESSED IN THIS AGREEMENT ARE THE ONLY TERMS UNDER WHICH BAY NETWORKS WILL PERMIT YOU TO USE THE SOFTWARE. If you do not accept these terms and conditions, return the product, unused and in the original shipping container, within 30 days of purchase to obtain a credit for the full purchase price.

1. License Grant. Bay Networks, Inc. ("Bay Networks") grants the end user of the Software ("Licensee") a personal, nonexclusive, nontransferable license: a) to use the Software either on a single computer or, if applicable, on a single authorized device identified by host ID, for which it was originally acquired; b) to copy the Software solely for backup purposes in support of authorized use of the Software; and c) to use and copy the associated user manual solely in support of authorized use of the Software by Licensee. This license applies to the Software only and does not extend to Bay Networks Agent software or other Bay Networks software products. Bay Networks Agent software or other Bay Networks software products are licensed for use under the terms of the applicable Bay Networks, Inc. Software License Agreement that accompanies such software and upon payment by the end user of the applicable license fees for such software.

2. Restrictions on use; reservation of rights. The Software and user manuals are protected under copyright laws. Bay Networks and/or its licensors retain all title and ownership in both the Software and user manuals, including any revisions made by Bay Networks or its licensors. The copyright notice must be reproduced and included with any copy of any portion of the Software or user manuals. Licensee may not modify, translate, decompile, disassemble, use for any competitive analysis, reverse engineer, distribute, or create derivative works from the Software or user manuals or any copy, in whole or in part. Except as expressly provided in this Agreement, Licensee may not copy or transfer the Software or user manuals, in whole or in part. The Software and user manuals embody Bay Networks' and its licensors' confidential and proprietary intellectual property. Licensee shall not sublicense, assign, or otherwise disclose to any third party the Software, or any information about the operation, design, performance, or implementation of the Software and user manuals that is confidential to Bay Networks and its licensors; however, Licensee may grant permission to its consultants, subcontractors, and agents to use the Software at Licensee's facility, provided they have agreed to use the Software only in accordance with the terms of this license.

3. Limited warranty. Bay Networks warrants each item of Software, as delivered by Bay Networks and properly installed and operated on Bay Networks hardware or other equipment it is originally licensed for, to function substantially as described in its accompanying user manual during its warranty period, which begins on the date Software is first shipped to Licensee. If any item of Software fails to so function during its warranty period, as the sole remedy Bay Networks will at its discretion provide a suitable fix, patch, or workaround for the problem that may be included in a future Software release. Bay Networks further warrants to Licensee that the media on which the Software is provided will be free from defects in materials and workmanship under normal use for a period of 90 days from the date Software is first shipped to Licensee. Bay Networks will replace defective media at no charge if it is returned to Bay Networks during the warranty period along with proof of the date of shipment. This warranty does not apply if the media has been damaged as a result of accident, misuse, or abuse. The Licensee assumes all responsibility for selection of the Software to achieve Licensee's intended results and for the installation, use, and results obtained from the Software. Bay Networks does not warrant a) that the functions contained in the software will meet the Licensee's requirements, b) that the Software will operate in the hardware or software combinations that the Licensee may select, c) that the operation of the Software will be uninterrupted or error free, or d) that all defects in the operation of the Software will be corrected. Bay Networks is not obligated to remedy any Software defect that cannot be reproduced with the latest Software release. These warranties do not apply to the Software if it has been (i) altered, except by Bay Networks or in accordance with its instructions; (ii) used in conjunction with another vendor's product, resulting in the defect; or (iii) damaged by improper environment, abuse, misuse, accident, or negligence. THE FOREGOING WARRANTIES AND LIMITATIONS ARE EXCLUSIVE REMEDIES AND ARE IN LIEU OF ALL OTHER WARRANTIES EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION ANY WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Licensee is responsible for the security of

its own data and information and for maintaining adequate procedures apart from the Software to reconstruct lost or altered files, data, or programs.

4. Limitation of liability. IN NO EVENT WILL BAY NETWORKS OR ITS LICENSORS BE LIABLE FOR ANY COST OF SUBSTITUTE PROCUREMENT; SPECIAL, INDIRECT, INCIDENTAL, OR CONSEQUENTIAL DAMAGES; OR ANY DAMAGES RESULTING FROM INACCURATE OR LOST DATA OR LOSS OF USE OR PROFITS ARISING OUT OF OR IN CONNECTION WITH THE PERFORMANCE OF THE SOFTWARE, EVEN IF BAY NETWORKS HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. IN NO EVENT SHALL THE LIABILITY OF BAY NETWORKS RELATING TO THE SOFTWARE OR THIS AGREEMENT EXCEED THE PRICE PAID TO BAY NETWORKS FOR THE SOFTWARE LICENSE.

5. Government Licensees. This provision applies to all Software and documentation acquired directly or indirectly by or on behalf of the United States Government. The Software and documentation are commercial products, licensed on the open market at market prices, and were developed entirely at private expense and without the use of any U.S. Government funds. The license to the U.S. Government is granted only with restricted rights, and use, duplication, or disclosure by the U.S. Government is subject to the restrictions set forth in subparagraph (c)(1) of the Commercial Computer Software—Restricted Rights clause of FAR 52.227-19 and the limitations set out in this license for civilian agencies, and subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause of DFARS 252.227-7013, for agencies of the Department of Defense or their successors, whichever is applicable.

6. Use of Software in the European Community. This provision applies to all Software acquired for use within the European Community. If Licensee uses the Software within a country in the European Community, the Software Directive enacted by the Council of European Communities Directive dated 14 May, 1991, will apply to the examination of the Software to facilitate interoperability. Licensee agrees to notify Bay Networks of any such intended examination of the Software and may procure support and assistance from Bay Networks.

7. Term and termination. This license is effective until terminated; however, all of the restrictions with respect to Bay Networks' copyright in the Software and user manuals will cease being effective at the date of expiration of the Bay Networks copyright; those restrictions relating to use and disclosure of Bay Networks' confidential information shall continue in effect. Licensee may terminate this license at any time. The license will automatically terminate if Licensee fails to comply with any of the terms and conditions of the license. Upon termination for any reason, Licensee will immediately destroy or return to Bay Networks the Software, user manuals, and all copies. Bay Networks is not liable to Licensee for damages in any form solely by reason of the termination of this license.

8. Export and Re-export. Licensee agrees not to export, directly or indirectly, the Software or related technical data or information without first obtaining any required export licenses or other governmental approvals. Without limiting the foregoing, Licensee, on behalf of itself and its subsidiaries and affiliates, agrees that it will not, without first obtaining all export licenses and approvals required by the U.S. Government: (i) export, re-export, transfer, or divert any such Software or technical data, or any direct product thereof, to any country to which such exports or re-exports are restricted or embargoed under United States export control laws and regulations, or to any national or resident of such restricted or embargoed countries; or (ii) provide the Software or related technical data or information to any military end user or for any military end use, including the design, development, or production of any chemical, nuclear, or biological weapons.

9. General. If any provision of this Agreement is held to be invalid or unenforceable by a court of competent jurisdiction, the remainder of the provisions of this Agreement shall remain in full force and effect. This Agreement will be governed by the laws of the state of California.

Should you have any questions concerning this Agreement, contact Bay Networks, Inc., 4401 Great America Parkway, P.O. Box 58185, Santa Clara, California 95054-8185.

LICENSEE ACKNOWLEDGES THAT LICENSEE HAS READ THIS AGREEMENT, UNDERSTANDS IT, AND AGREES TO BE BOUND BY ITS TERMS AND CONDITIONS. LICENSEE FURTHER AGREES THAT THIS AGREEMENT IS THE ENTIRE AND EXCLUSIVE AGREEMENT BETWEEN BAY NETWORKS AND LICENSEE, WHICH SUPERSEDES ALL PRIOR ORAL AND WRITTEN AGREEMENTS AND COMMUNICATIONS BETWEEN THE PARTIES PERTAINING TO THE SUBJECT MATTER OF THIS AGREEMENT. NO DIFFERENT OR ADDITIONAL TERMS WILL BE ENFORCEABLE AGAINST BAY NETWORKS UNLESS BAY NETWORKS GIVES ITS EXPRESS WRITTEN CONSENT, INCLUDING AN EXPRESS WAIVER OF THE TERMS OF THIS AGREEMENT.

Contents

Preface

Before You Begin xi
Text Conventions xii
Acronyms xiii
Bay Networks Technical Publications xiv
How to Get Help xv

Chapter 1
VINES Overview

VINES Networks 1-1
VINES Architecture 1-2
VINES Network Addressing 1-4
How the Router for VINES Services Works 1-6
VINES Data Link Protocols 1-7
VINES Routing Protocols 1-8
VINES Internet Protocol 1-8
VINES Nonsequenced Routing Update Protocol 1-10
VINES Sequenced Routing Update Protocol 1-14
VINES Nonsequenced Address Resolution Protocol 1-15
VINES Sequenced Address Resolution Protocol 1-16
VINES Internet Control Protocol 1-16
For More Information 1-17

Chapter 2
VINES Implementation Notes

Enabling VINES on a Synchronous Line 2-1
Using the Inverse Address Resolution Protocol for VINES Internet Address Resolution 2-2
Assigning a Network ID to Your Router 2-2

Configuring Routers for Serverless Network Segments 2-2
VINES Security Limitation for Serverless Network Segments 2-3
Configuring Routers for Multiple-Hop Topologies 2-3
Configuring Routers to Source Route over Token Ring Networks 2-4
Making the Transition from Bridging VINES to Routing VINES 2-5
Fragmentation Protocol and VINES Performance 2-7
Help Thy Neighbor Support 2-7
Using Multipath with Load Sharing 2-8
Partially Meshed Frame Relay Network Support 2-8
Avoiding Address Numbering Problems in LNs and CNs 2-9

Chapter 3
Enabling VINES Services

Enabling VINES on an Interface 3-1

Chapter 4
Editing VINES Parameters

Accessing VINES Parameters 4-2
Editing VINES Global Parameters 4-3
VINES Global Parameter Descriptions 4-3
Editing VINES Interface Parameters 4-7
VINES Interfaces Parameter Descriptions 4-8
Deleting VINES from the Router 4-14

Appendix A
VINES Default Settings

Index

Figures

Figure 1-1. VINES Server and Its Clients 1-2
Figure 1-2. VINES Network 1-5
Figure 1-3. VINES Internet Address Format 1-6
Figure 1-4. VINES Fragmentation Protocol Header 1-7
Figure 1-5. VINES Internet Protocol Header 1-9
Figure 1-6. VINES Nonsequenced Routing Update Protocol Header 1-11
Figure 1-7. VINES Nonsequenced Address Resolution Protocol Header 1-15
Figure 1-8. VINES Internet Control Protocol Header 1-16
Figure 2-1. Routers Configured on a Serverless Network Segment 2-3
Figure 2-2. Source Routing Across a Token Ring Network 2-5
Figure 2-3. Configuring Multiple Loops in a Bridged Environment 2-6
Figure 3-1. Edit Interface Details Window 3-2
Figure 3-2. Edit Connector Window 3-3
Figure 3-3. Edit SYNC Parameters Window 3-3
Figure 4-1. Configuration Manager Window 4-2
Figure 4-2. Edit VINES Global Parameters Window 4-3
Figure 4-3. VINES Interfaces Window 4-7

Tables

Table 1-1. VINES Protocol Stack 1-2
Table 1-2. Assignment of Subnetwork Numbers 1-6
Table 1-3. VINES Routing Tables 1-12
Table 4-1. Broadcast Class Options 4-5
Table A-1. VINES Global Parameters A-1
Table A-2. VINES Interface Parameters A-2

Preface

This guide describes the Virtual Networking System (VINES) and what you do to start and customize VINES services on a Bay Networks® router.

Before You Begin

Before using this guide, you must complete the following procedures. For a new router:

- Install the router (refer to the installation manual that came with your router).
- Connect the router to the network and create a pilot configuration file (refer to *Quick-Starting Routers*, *Configuring BayStack Remote Access*, or *Connecting ASN Routers to a Network)*.

Make sure that you are running the latest version of Bay Networks BayRS™ and Site Manager software. For information about upgrading BayRS and Site Manager, see the upgrading guide for your version of BayRS.

Text Conventions

This guide uses the following text conventions:

angle brackets (< >)	Indicate that you choose the text to enter based on the description inside the brackets. Do not type the brackets when entering the command. Example: If the command syntax is: **ping** *<ip_address>*, you enter: **ping 192.32.10.12**
bold text	Indicates text that you need to enter and command names and options. Example: Enter **show ip** {**alerts** | **routes**} Example: Use the **dinfo** command.
braces ({})	Indicate required elements in syntax descriptions where there is more than one option. You must choose only one of the options. Do not type the braces when entering the command. Example: If the command syntax is: **show ip** {**alerts** | **routes**}, you must enter either: **show ip alerts** or **show ip routes**.
brackets ([ ])	Indicate optional elements in syntax descriptions. Do not type the brackets when entering the command. Example: If the command syntax is: **show ip interfaces** [**-alerts**], you can enter either: **show ip interfaces** or **show ip interfaces -alerts**.
ellipsis points (. . .)	Indicate that you repeat the last element of the command as needed. Example: If the command syntax is: **ethernet/2/1** [<*parameter*> <*value*>] . . ., you enter **ethernet/2/1** and as many parameter-value pairs as needed.

italic text	Indicates file and directory names, new terms, book titles, and variables in command syntax descriptions. Where a variable is two or more words, the words are connected by an underscore. Example: If the command syntax is: **show at** <*valid_route*> *valid_route* is one variable and you substitute one value for it.
`screen text`	Indicates system output, for example, prompts and system messages. Example: `Set Bay Networks Trap Monitor Filters`
separator (>)	Shows menu paths. Example: Protocols > IP identifies the IP option on the Protocols menu.
vertical line (|)	Separates choices for command keywords and arguments. Enter only one of the choices. Do not type the vertical line when entering the command. Example: If the command syntax is: **show ip** {**alerts** | **routes**}, you enter either: **show ip alerts** or **show ip routes**, but not both.

Acronyms

ARP	Address Resolution Protocol
HDLC	High-level Data Link Control
ICMP	Internet Control Message Protocol
ICP	Internet Control Protocol
IPC	Interprocess Communication
IEEE	Institute of Electrical and Electronic Engineers
IP	Internet Protocol
ISO	International Organization for Standardization
MAC	media access control

OSI	Open Systems Interconnection
RTP	Routing Update Protocol
SMDS	Switched Multimegabit Data Services
SNAP	Subnetwork Access Protocol
SPP	Sequenced Packet Protocol
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
VINES	Virtual Networking System

Bay Networks Technical Publications

You can now print Bay Networks technical manuals and release notes free, directly from the Internet. Go to *support.baynetworks.com/library/tpubs/*. Find the Bay Networks product for which you need documentation. Then locate the specific category and model or version for your hardware or software product. Using Adobe Acrobat Reader, you can open the manuals and release notes, search for the sections you need, and print them on most standard printers. You can download Acrobat Reader free from the Adobe Systems Web site, *www.adobe.com*.

You can purchase Bay Networks documentation sets, CDs, and selected technical publications through the Bay Networks Collateral Catalog. The catalog is located on the World Wide Web at *support.baynetworks.com/catalog.html* and is divided into sections arranged alphabetically:

- The “CD ROMs” section lists available CDs.
- The “Guides/Books” section lists books on technical topics.
- The “Technical Manuals” section lists available printed documentation sets.

Make a note of the part numbers and prices of the items that you want to order. Use the “Marketing Collateral Catalog description” link to place an order and to print the order form.

How to Get Help

For product assistance, support contracts, or information about educational services, go to the following URL:

http://www.baynetworks.com/corporate/contacts/

Or telephone the Bay Networks Technical Solutions Center at:

800-2LANWAN

Chapter 1
VINES Overview

This overview of the Virtual Networking System (VINES) looks briefly at

- VINES network organization, architecture, and addressing scheme
- Router software for VINES services, including the data link and routing protocols

VINES Networks

Banyan Systems developed VINES as a network for personal computers. Based on UNIX System 5.3, VINES uses a distributed system environment wherein PC users easily communicate and share hardware (such as printers, disk space, and modems) and software (such as files and applications) transparently on a network.

To a PC user, VINES presents a complex, multivendor network as if it were a single-vendor network. Resources from all servers on the network are available to individual PCs with system administrators controlling access to those resources.

A VINES network employs servers, clients, and various communications hardware connected over LANs and WANs (Figure 1-1):

- *Servers* are computers that run VINES server software to provide connectivity and services, such as file and print services, to PC users. Banyan and several other vendors manufacture VINES server hardware.
- *Clients* are PCs that run VINES client software and use the services provided by servers.

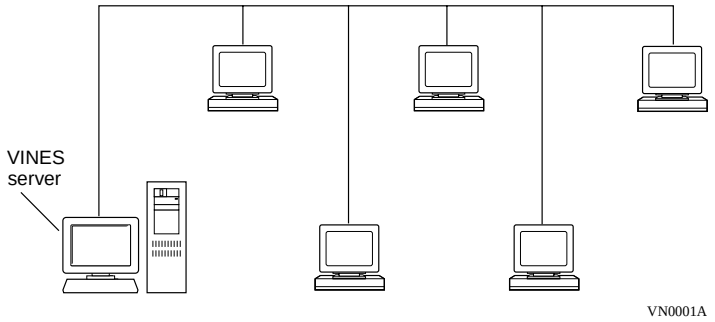

Figure 1-1. VINES Server and Its Clients

Datagrams called *VINES internet packets* carry information across a VINES environment. Within each packet is the source and destination address needed to route the packet between nodes on the network. Each packet is a discrete unit of data that travels independently on the network layer.

VINES Architecture

VINES architecture reflects the International Organization for Standardization (ISO) for Open Systems Interconnection (OSI). Banyan designed VINES to support both existing and future OSI model requirements. The VINES protocol stack has seven layers; the lower three layers deliver and route data, while the upper layers handle application-specific processes (Table 1-1).

Table 1-1. VINES Protocol Stack

Layer	Protocol or Application
Application	VINES services, VINES Tasker, UNIX, DOS, and StreetTalk
Presentation	VINES Matchmaker Data Type Representations
Session	VINES Matchmaker Remote Procedure Calls

(continued)

Table 1-1. VINES Protocol Stack *(continued)*

Layer	Protocol or Application
Transport	VINES Interprocess Communication (IPC) Protocol VINES Sequenced Packet Protocol (SPP), Transmission Control Protocol (TCP), and User Datagram Protocol (UDP)
Network	VINES Internet Protocol (IP) VINES Internet Control Protocol (ICP) VINES Nonsequenced Address Resolution Protocol (ARP) VINES Sequenced ARP VINES Nonsequenced Routing Update Protocol (RTP) VINES Sequenced RTP X.25, X.3, X.29, and IP used by TCP, ICMP, and NetBIOS
Data Link	VINES Fragmentation Protocol Drivers for Block Asynchronous, High Data Link Control (HDLC), Token Ring, Ethernet, other LANS, and Institute of Electrical and Electronic Engineers (IEEE) 802.x standards
Physical	Broadband, baseband, point-to-point, and twisted pair

At the data link level, VINES currently supports several IEEE standards, including Ethernet, Token Ring, and 802.x. VINES also provides its own proprietary data link protocol, VINES Fragmentation Protocol, which breaks up and reassembles packets that are too large to travel over certain media. However, only routers configured over synchronous lines support VINES Fragmentation Protocol.

At the networking level, VINES supports both industry standard protocols such as TCP/IP, X.25, and AppleTalk, and its own set of networking protocols. The latter include VINES

- Internet Protocol
- Nonsequenced Routing Update Protocol
- Sequenced Routing Update Protocol
- Nonsequenced Address Resolution Protocol
- Sequenced Address Resolution Protocol
- Internet Control Protocol

Upper-layer protocols include VINES print and file service applications and the VINES naming protocol, StreetTalk.

StreetTalk is a distributed directory service that contains the names and attributes of all critical network resources. Each resource on a VINES network has a StreetTalk name that is globally unique.

StreetTalk names have the following format:

item@group@organization

where

item identifies a user or resource on the network.
group identifies the group to which the item belongs.
organization identifies the organization to which the group belongs.

VINES adapts to changes in the network topology; because the VINES network refers to each resource by name, you can move or replace it and the PCs can still locate it. System administrators control which resources end users on the network can access.

VINES Network Addressing

Each node grouping on a VINES network consists of a service node and the client nodes to which the service node provides address resolution and routing services (Figure 1-2). Note that this is a logical grouping; client nodes may or may not map directly to the same physical media.

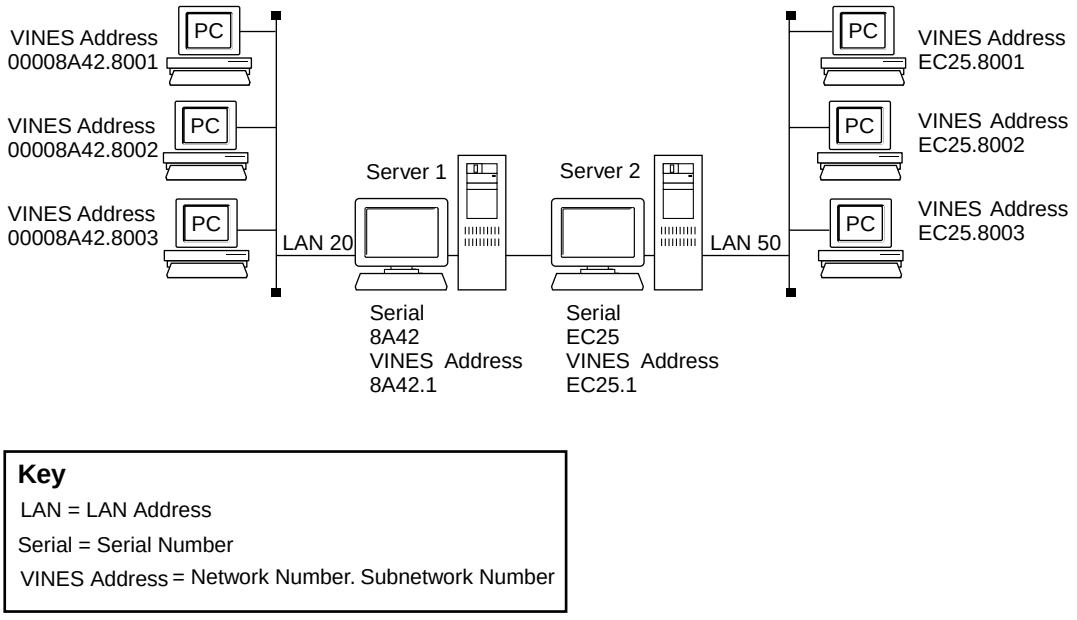

Figure 1-2. VINES Network

When a client node becomes active on the network, it broadcasts a query request to all servers. All reachable servers respond. The client node chooses the first server that responds and requests a VINES internet address from that server. The service node assigns a unique, 48-bit VINES internet address to the client node.

The VINES internet address is independent of any data-link-layer address assigned to a node on a physical medium. The 48-bit VINES internet address consists of two fields (Figure 1-3):

- The 32-bit network number field

  The network number is the serial number of the server node and identifies the logical grouping of nodes on a VINES network.

- The 16-bit subnetwork number field

  The subnetwork number identifies the node within the server node's logical grouping.

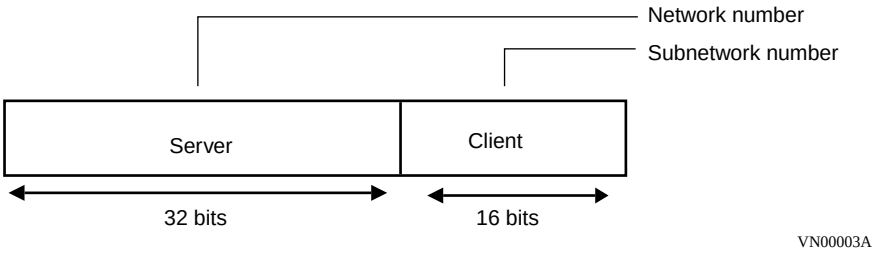

Figure 1-3. VINES Internet Address Format

The internet address for each service node in a VINES network is its network number, integrated with the subnetwork number 1. The service node assigns unique internet addresses to all other client nodes in its subnetwork by integrating its network number with a unique subnetwork number for each node. The service node assigns subnetwork numbers as shown in Table 1-2.

Table 1-2. Assignment of Subnetwork Numbers

Subnetwork Number	Node Type
1	Server only
2 to 0x7fff	Unused
0x8001 to 0xfffe	Clients only
ffff	Broadcast

How the Router for VINES Services Works

On a VINES network, the router maintains the network topology and uses both IEEE standard and VINES proprietary protocols to route packets through the network. The router supplies client nodes with addresses only if there are no other servers on the network.

The following sections describe the VINES data link and routing protocols that the router uses.

VINES Data Link Protocols

The VINES data link protocols support the exchange and broadcast of data frames between neighboring server and client nodes on the network. The maximum frame size is 1500 bytes.

In addition to supporting most of the IEEE standards, the VINES Fragmentation Protocol breaks up packets that are too large to travel over certain media into smaller-sized frames and reassembles them. However, the Fragmentation Protocol supports routers configured over synchronous lines only. For example, if a node on an IBM PC LAN attempts to send a packet to a node on an Ethernet LAN over a synchronous network, the Fragmentation Protocol fragments the packet into smaller-sized frames. This enables the router to transport the packets over an Ethernet LAN.

The Fragmentation Protocol has a 2-byte header that stores information and follows the data link header in a VINES frame (Figure 1-4).

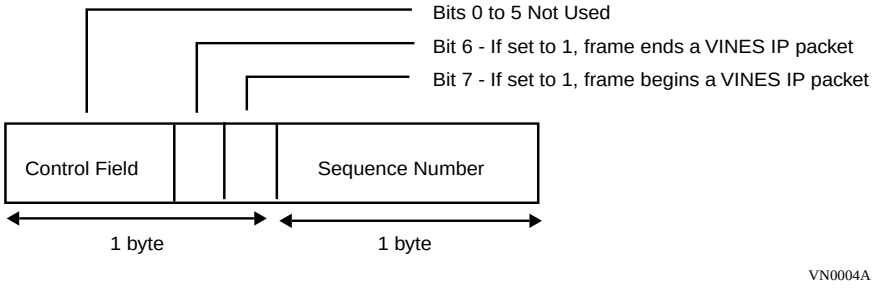
Bits 0 to 5 Not Used
Bit 6 - If set to 1, frame ends a VINES IP packet
Bit 7 - If set to 1, frame begins a VINES IP packet
Control Field
Sequence Number
1 byte
1 byte
VN0004A

Figure 1-4. VINES Fragmentation Protocol Header

The first byte of the header contains a control field and the second byte contains a sequence number. The value of the control field indicates whether the frame begins or ends in a VINES IP packet. Only the first fragment includes the VINES IP header.

The value of the sequence number field is modulo 256. The node that originated the frame determines this value. The receiving node uses this value to determine the correct order in which to reassemble the data packet as it receives fragments. If the receiving node receives the fragments out of order, the intermediate node discards all fragments and the partially reassembled packet.

VINES Routing Protocols

The VINES network layer protocols route VINES data packets to destination nodes using the fastest route available. They also distribute the current network topology throughout the network. The VINES network layer supports connectionless (datagram) services only. The maximum packet length on a VINES network is 1500 bytes, including the VINES Internet Protocol header.

The following sections describe our implementation of the VINES networking protocols. These include VINES

- Internet Protocol
- Nonsequenced Routing Update Protocol
- Sequenced Routing Update Protocol
- Nonsequenced Address Resolution Protocol
- Sequenced Address Resolution Protocol
- Internet Control Protocol

VINES Internet Protocol

VINES Internet Protocol (IP) routes packets from the source node to the destination node. The IP packet header specifies the destination node's internet address. All internet packets begin with a VINES IP header that identifies the source and destination node addresses, and contains an identifier for the next protocol in the packet, a transport control byte, the length of the entire packet, and a software checksum, if needed. A header for another network layer protocol or transport layer protocol follows the VINES IP header (Figure 1-5).

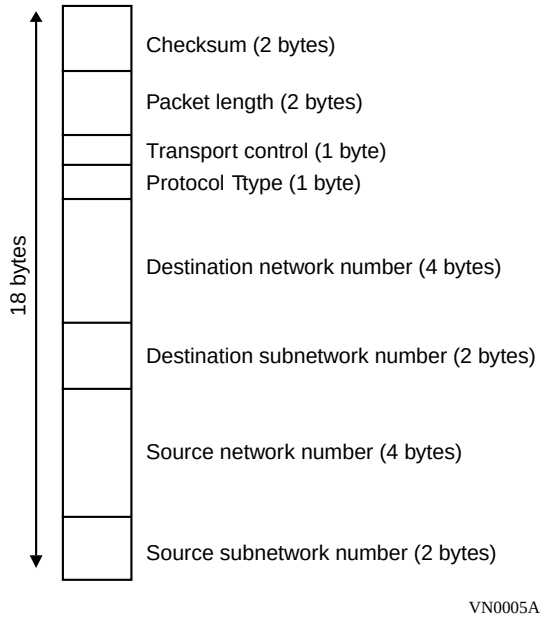

Figure 1-5. VINES Internet Protocol Header

When the router receives a packet, the VINES IP entity on the router handles the packet according to how it is addressed, as follows:

- Packets destined for the router

  When the router receives a packet addressed to itself, it first reassembles the packet, if it is fragmented. Next, the router ensures that the packet is not corrupted by checking the checksum, if there is one. Finally, it passes the packet up to the next level for processing.

- Broadcast packets

  When the router receives a broadcast packet, it checks the packet's hop count to ensure that it is not zero. In most cases, if the hop count is zero, the router discards the packet (unless it is a StreetTalk or Time Sync Service packet). If the node accepts the packet, the router decrements the hop count by one before retransmitting the packet on all interfaces except for the one that received it.

If the broadcast packet is a *StreetTalk broadcast packet*, which propagates StreetTalk information, or a *Time Sync Service broadcast packet*, which propagates time information, the router ignores the hop count. First, the router checks to see if the interface that provides the best path back to the originating node received the packet. If it did, the router retransmits the packet on all other interfaces (without modifying the hop-count field). Otherwise, the router determines that the packet has looped back, and discards it.

The router recognizes a StreetTalk broadcast packet or a Time Sync Service broadcast packet by examining the destination port field of the packet's ICP header. The router sets the destination port field to 0x0000f for all StreetTalk packets and 0x0007 for all Time Sync Service packets.

- Nonbroadcast packets

  When the router receives a nonbroadcast packet with a different destination address, the router must forward the packet. First, it reassembles the packet, if necessary. Then, it refers to its next hop routing table to determine the next hop. Finally, it forwards the packet to this hop.

VINES Nonsequenced Routing Update Protocol

The VINES Nonsequenced Routing Update Protocol (Nonsequenced RTP) maintains a local routing table that VINES IP can refer to when it selects paths. Nonsequenced RTP also distributes this information about the network topology among the servers and clients in the network. Nonsequenced RTP packets have a 4-byte header that immediately follows the VINES IP header (Figure 1-6).

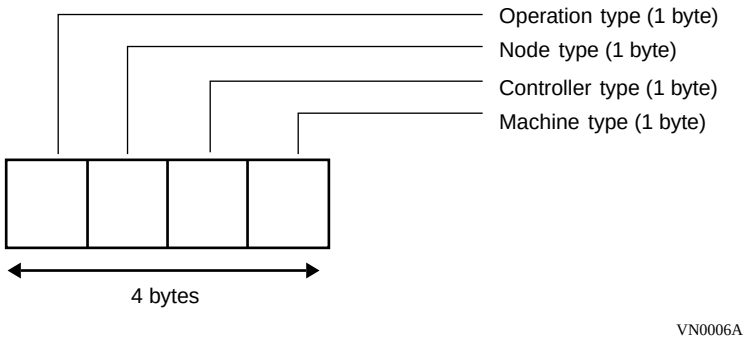

Figure 1-6. VINES Nonsequenced Routing Update Protocol Header

The four fields of the header are as follows:

- *Operation type specifies the packet type:* routing request, update, or redirect or response.
- *Node type* specifies the type of node that originated the packet: service or client.
- *Controller type* specifies the type of controller that originated the packet: single-buffer or multibuffer LAN card.
- *Machine type* specifies the type of processor that originated the packet.

Nonsequenced RTP distinguishes between service nodes and client nodes on the network. Service nodes route packets addressed to other nodes, usually servers. Client nodes do not perform any routing services. Both service nodes and client nodes maintain two routing tables: a *table of all known networks* and a *table of neighbors.* When you configure both Nonsequenced RTP and Sequenced RTP on the router, the protocols share these routing tables (Table 1-3).

Table 1-3. VINES Routing Tables

Table Entry	Contents
Table of Networks	Network number
	Network sequence number* This equals 0 for nonsequenced routes.
	Timestamped sequence number*
	Routing metric to reach the network
	Sequenced advertised metric*
	Next hop used to reach the network
Table of Neighbors	Network number
	Subnetwork number
	Sequence number* This equals 0 for nonsequenced neighbors.
	Medium over which the packet can reach the neighbor
	LAN address of neighbor
	Routing metric used to reach the neighbor
	Sequenced advertised metric*

*Used for Sequenced RTP only.

For service nodes, the table of networks contains an entry for all known networks, except for the server's own. Client nodes keep track only of the networks with which they are currently communicating, thus reducing table space. For service nodes, the table of neighbors contains an entry for each neighboring node. Client nodes keep track only of the neighbors with which they are currently communicating.

The Nonsequenced RTP entities exchange these four types of packets:

- Nonsequenced routing update packets

Every node on a VINES network periodically broadcasts nonsequenced routing update packets. Nodes on LAN and high-speed media send out nonsequenced routing update packets every 90 seconds. These packets inform neighbors of the node's existence and type. Routes remain in a neighbor's routing table for 6 minutes. If the neighbor does not hear from the node again within 6 minutes, the neighbor marks the route as unreachable and removes it from the routing table. The packets sent out by service nodes also include a list of all networks known to the service node and the cost of reaching these networks from that service node.

On server-to-server connectivity and over WAN connections (TCP/IP, X.25, HDLC, Block Asynchronous), service nodes send out five full, nonsequenced routing update packets when the node first comes up on the network. Afterwards, nonsequenced routing update packets are generated only when you make routing changes to the network. All routes permanently remain in a node's routing table for these types of connections.

- Nonsequenced routing request packets

  A client node generates nonsequenced routing request packets when it needs information about the network topology.

- Nonsequenced routing response packets

  In response to receiving a nonsequenced routing request packet, service nodes generate nonsequenced routing response packets that describe the network topology.

- Nonsequenced routing redirect packets

  A service node generates nonsequenced routing redirect packets when it determines that a better path exists for forwarding packets between nodes. The service node sends a nonsequenced routing redirect packet to the last hop that forwarded the packet, informing it of the existence of a better route. The service node also sends the original packet toward the destination.

VINES Sequenced Routing Update Protocol

VINES Sequenced Routing Update Protocol (Sequenced RTP) differs from Nonsequenced RTP in that routers identify routing information packets with sequence numbers. Each router on the network has a sequence number that it advertises to neighboring routers. The neighboring router uses the sequence numbers to determine if its routing table contains the most current and accurate routing information. Routers also use sequence numbers to time stamp changes in the network topology.

With Sequenced RTP, routers and servers in a network consisting of only VINES Version 5.50 devices do not perform periodic broadcasts of full routing tables; this reduces the network bandwidth usage. A router sends out routing table information only when

- A network topology change occurs
- Another router or client requests the information
- The network contains routers or servers configured for both Sequenced and Nonsequenced RTP

The router sends out the routing table information as sequenced routing update and sequenced routing response packets. (Refer to Table 1-3 for details about the routing tables and their contents.) Depending on the amount of information and the type of physical media, a single update or response can consist of one or more sequenced packets. Sequenced routing update and response packets have a 32-bit sequence number ranging from 0x0 to 0xffffffff.

Each time a change occurs to a router's local network topology, the router verifies the sequence number, records the information in its routing table, and broadcasts a sequenced routing update packet to its immediate neighbors. The packet contains the router's own sequence number incremented by one. This new sequence number indicates that the router is transmitting new routing table information.

VINES Sequenced RTP has the following advantages:

- Reduces network bandwidth usage (when you set the RTP Mode parameter to Sequenced RTP or Automode)
- Allows the router to interoperate with Banyan servers or clients running VINES Version 4.11 or Version 5.50 software

You can configure your VINES interface to support Sequenced RTP only, Nonsequenced RTP only, or Automode (both Sequenced RTP and Nonsequenced RTP), using the RTP Mode parameter. (Refer to Chapter 4 for details about using Site Manager to access this parameter.) However, if you configure the interface for Sequenced RTP only, the network connected to all of the interfaces must have Banyan Version 5.50 servers or clients. Likewise, if you configure the interface for Nonsequenced RTP only, the network must have Banyan Version 4.11 servers or clients.

In a mixed network, that is, one running both Sequenced and Nonsequenced RTP and configured for Automode, the router sends out a nonsequenced routing update packet only when it receives a nonsequenced routing update packet from a server, router, or client. Otherwise, the router advertises sequenced routing update packets only.

VINES Nonsequenced Address Resolution Protocol

The VINES Nonsequenced Address Resolution Protocol (Nonsequenced ARP) allows service nodes to provide address resolution services to client nodes that do not have VINES internet addresses. VINES uses the VINES IP services to deliver address resolution packets between nodes.

A VINES Nonsequenced ARP packet is prefixed with an 8-byte header and follows the VINES IP header (Figure 1-7).

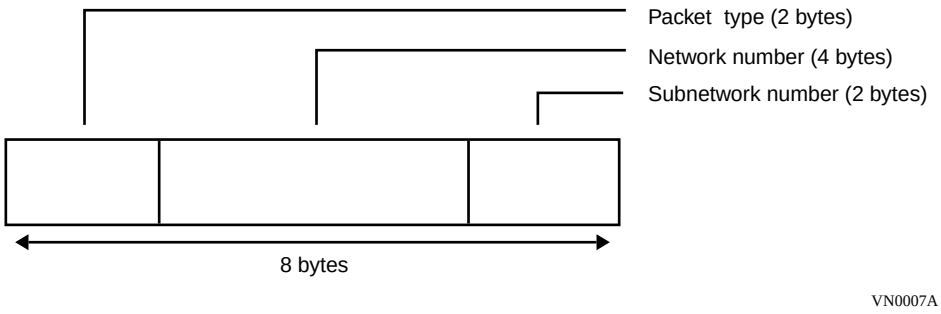

Figure 1-7. VINES Nonsequenced Address Resolution Protocol Header

VINES Nonsequenced ARP defines two types of entities:

- Address resolution services

Nodes that can route VINES packets and have a static, unique, 32-bit network number implement these services; they are usually service nodes.

- Address resolution clients

  Nodes that do not have a VINES address implement these clients; they are usually client nodes.

VINES Sequenced Address Resolution Protocol

VINES Sequenced Address Resolution Protocol (Sequenced ARP) works with Sequenced RTP. With VINES Sequenced ARP, a client receives an assignment response that includes the VINES address, sequence number, and metric of the routing server. The routers that receive the VINES 5.50 client Sequenced ARP requests or assignment requests will respond automatically with Sequenced ARP response packets.

You can disable or enable VINES ARP on a router, using the ARP Enable parameter. Refer to Chapter 4 for details about this parameter.

VINES Internet Control Protocol

VINES Internet Control Protocol (ICP) supports certain transport layer protocol entities by reporting network errors and topological conditions. A VINES ICP packet has a 4-byte header and follows the VINES IP header (Figure 1-8).

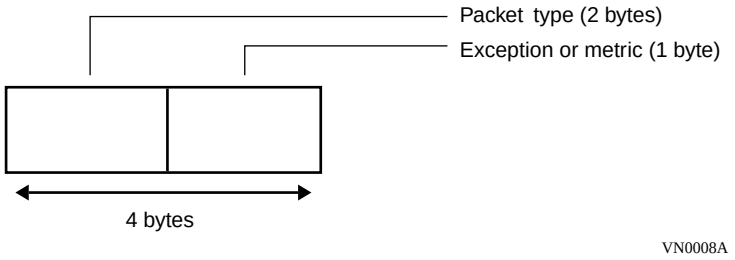

Figure 1-8. VINES Internet Control Protocol Header

The ICP entity generates these two types of ICP packets:

- Exception notification packets

These packets specify that network layer exceptions occurred during the routing of transport layer messages. The ICP entity generates exception notification packets when

-- VINES IP cannot properly route or receive a VINES IP packet. For example, a service node receives a packet containing an unknown destination address.

-- The packet has the error subfield enabled in the VINES IP header's transport control field.

- Metric notification packets

  These packets contain metric information about the final transmission medium used to reach a client node. The ICP entity generates metric notification packets when

  -- The entity routes a packet with the metric subfield enabled in the transport control field of the VINES IP header.

  -- The destination address in the VINES IP header specifies a node that is a neighbor of the service node.

For More Information

The following documents give technical detail on VINES protocol implementation:

VINES Architecture Definition. Banyan Systems Inc. April 1993.

VINES Protocol Definition. Banyan Systems Inc. June 1993.

Chapter 2
VINES Implementation Notes

This chapter contains Bay Networks specific implementation notes that you should keep in mind when you configure VINES services. It describes what you need to know if you want to

- Configure the router on a synchronous line.
- Use the Inverse ARP feature for internet address resolution.
- Assign a network ID to the router.
- Configure the router on a serverless network segment or to source route over Token Ring networks.
- Make the transition from bridging to routing VINES.
- Enable or disable the VINES Fragmentation Protocol (FRP) header.
- Use the multipath with load sharing feature.
- Avoid VINES address numbering problems on Bay Networks LN and CN routers.

Enabling VINES on a Synchronous Line

If you want to route VINES packets over synchronous protocols, such as Standard Sync, Frame Relay, Point-to-Point, Switched Multimegabit Data Services (SMDS), or Asynchronous Transfer Mode (ATM), you must enable VINES support on a synchronous line. To do this, you must specify two synchronous line parameters:

- Clocking source (internal or external)
- Synchronous line speed

For information on specifying values for these two parameters, refer to "Enabling VINES on an Interface" in Chapter 3.

Using the Inverse Address Resolution Protocol for VINES Internet Address Resolution

You use VINES Inverse ARP to determine the VINES internet address of the neighboring router on the other end of a virtual circuit in a Frame Relay or ATM network. When a new virtual circuit comes up on the Frame Relay or ATM interface, the VINES software sends an Inverse ARP request with its VINES internet address to this data link connection. The router on the other end of the new data link connection responds with an Inverse ARP response, which includes the VINES internet address of its neighbor. When the original router receives the request, it learns the new neighbor's internet address.

Assigning a Network ID to Your Router

When you enable VINES on the router, we recommend that you accept the default network ID. The router uses its system controller's serial number to calculate the network ID. This guarantees that the number is unique.

However, if you choose to specify a different network ID, make sure the number you assign is unique within the VINES network; refer to "Editing VINES Global Parameters" in Chapter 4 for details on enabling the network ID parameter.

Configuring Routers for Serverless Network Segments

If you enable VINES on a circuit that contains no VINES servers, then you must enable VINES ARP on the circuit, so that the router can provide address resolution services to client nodes on this circuit.

You enable ARP using the ARP Enable parameter; refer to "Editing VINES Interface Parameters" in Chapter 4 for details on enabling this parameter.

VINES Security Limitation for Serverless Network Segments

VINES login location restriction is a security feature that limits the client's login capability, using a specific LAN segment. This feature does not work on a serverless circuit.

A VINES server specifies a LAN segment, using the server name and slot number. The router has no server name, so it cannot name the segment. When the client attempts to log in to the router, the login fails.

Configuring Routers for Multiple-Hop Topologies

If your VINES network topology has two or more hops between client nodes and the server that services the circuit, you must

- Set the circuit's ARP Enable parameter to Enable so that the VINES router can provide address resolution services to any client nodes.
- Set the Remote Client Privileges parameter to Enable on those circuits that connect the routers to the server. This allows the client nodes to communicate with the server, even though they are separated by more than one hop.

Note: When you enable the Remote Client Privileges parameter, you automatically enable the Serverless Networks for WANs parameter. Banyan does not recommend using serverless networks on a WAN because the high cost increases delays and may terminate sessions. We, however, do support this configuration.

Figure 2-1 shows a sample VINES network in which the VINES server is separated from the client nodes by two routers.

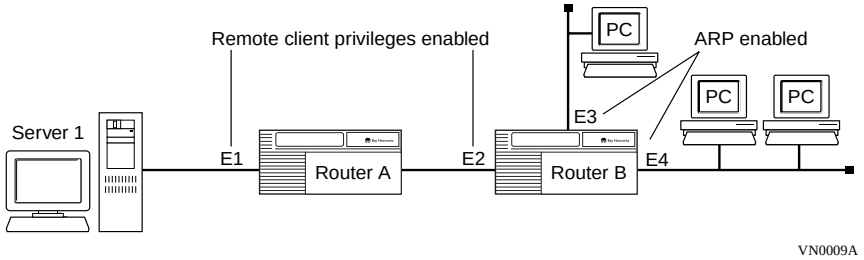

Figure 2-1. Routers Configured on a Serverless Network Segment

For the server and client nodes to communicate, we configured the routers in this way:

- Enabled VINES on circuits E1, E2, E3, E4
- Set the ARP Enable parameter to Enable on circuits E3 and E4 so that Router B can provide address resolution services to the client nodes on these circuits
- Set the Remote Client Privileges parameter to Enable on circuits E1 and E2, so that the client nodes on circuits E3 and E4 can reach the server via Routers A and B

As a result, the server and client nodes on this network can communicate, even though they are separated by more than one hop.

Configuring Routers to Source Route over Token Ring Networks

The router configured for VINES services can route over Token Ring networks that contain one or more source-routing bridges. In a source-routing network, every endstation that sends out a frame supplies the frame with the necessary route descriptors so that it can be source routed across the network. Thus, for VINES routers to route packets across a source-routing network, they must act like endstations. That is, they must supply route descriptors for each packet before they send it out onto the network.

With end-node support enabled, whenever a router running VINES receives a packet and determines that the packet's next hop is located across a source-routing network, the router does the following:

- Adds the necessary RIF information to the packet's MAC header
- Sends the packet out onto the network where it is source routed toward the next hop

Upon receiving the packet from the Token Ring network, the peer router strips off the RIF field and continues to route the packet toward the destination network address (Figure 2-2).

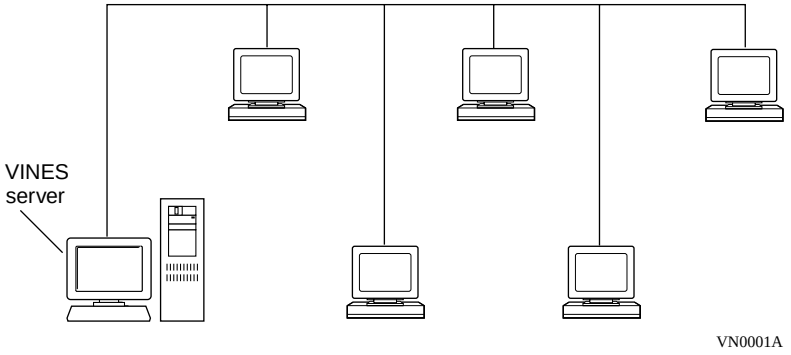

Figure 2-2. Source Routing Across a Token Ring Network

You configure source routing end-node support on a per-circuit basis by setting the End Station Enable parameter to Enable. Refer to "Editing VINES Interface Parameters" in Chapter 4 for details on enabling this parameter.

Making the Transition from Bridging VINES to Routing VINES

If you want to shift from bridging to routing VINES over WANs, you must temporarily disable the Fragmentation Protocol (FRP) header on each VINES WAN interface connected to a bridge.

Note: You may also need to disable the FRP header for your router to interoperate with other routers that do not support the Fragmentation Protocol.

To disable the FRP header, disable the Use of FRP Header parameter; the default value of this parameter is Enable. Refer to "Editing VINES Interface Parameters" in Chapter 4 for details on disabling this parameter.

For example, Figure 2-3 shows multiple loops in a bridged environment.

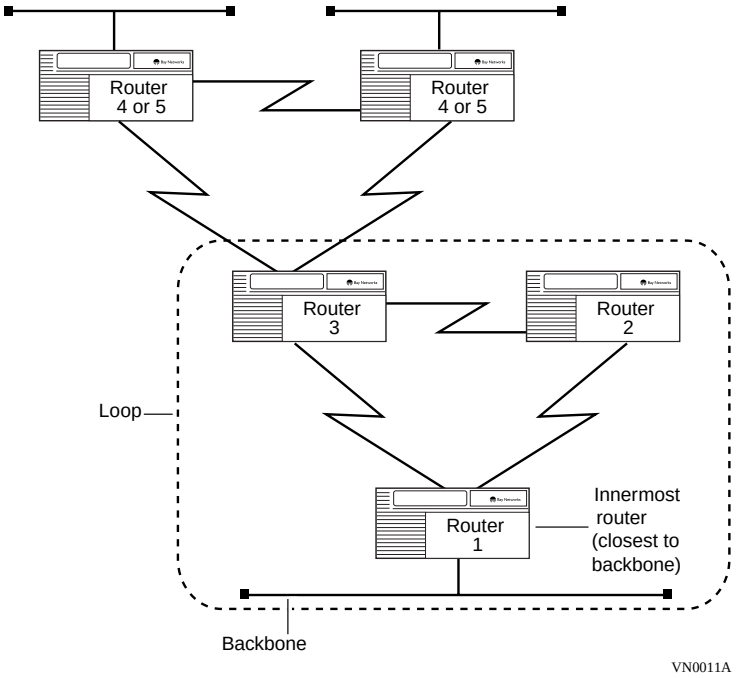

Figure 2-3. Configuring Multiple Loops in a Bridged Environment

You must make the transition to VINES routing from the innermost loop first, and then move outward. To do this:

1. **Use Site Manager to select the router in the loop that is connected to the backbone.**
2. **Enable VINES on the interfaces you want.**

   Refer to Chapter 3 for details on enabling VINES.
3. **Select Protocols > Vines > Interfaces from the Configuration Manager window.**

   The Edit Vines Interface window appears.
4. **Disable the Use of FRP Header parameter on all VINES WAN interfaces that are connected to routers that are bridging only. If there is a router in the loop that is not connected to another loop, select that router next. Then repeat Steps 2 to 4.**

A router connected to another loop should be the last router you configure in that loop (Router 3 in Figure 2-3). The numbers shown in the routers in Figure 2-3 indicate the order in which you should configure the routers. Note that with Router 4 or 5, it does not matter which one you configure first because neither one connects to another loop.

5. **Enable the Use of FRP Header parameter on all the WAN interfaces after you configure all routers in the loops, and they are routing with VINES enabled.**

Fragmentation Protocol and VINES Performance

The setting of the VINES FRP header affects how VINES services perform. Specifically, enabling or disabling the FRP header affects the maximum forwarding rate and throughput. When the FRP header is enabled, the default, forwarding rate and throughput slow down. When you disable the FRP header, performance of these factors improves.

It is not necessary to enable the FRP header on all WAN links. Enabling fragmentation is appropriate for low speed WAN links. You do not need to use the FRP header on high speed links where the MTU setting is 1500 bytes (the default setting).

If you experience performance bottlenecks over a WAN link (especially over a higher speed WAN link) using VINES, disable the use of FRP header on the VINES interface on *both sides* of the WAN link. For information on changing the FRP Header parameter, refer to "Editing VINES Interface Parameters" in Chapter 4.

Note: Changing the default for FRP to Disabled in routers running Version 8.10 may cause backward compatibility problems, if the router on the other end of a WAN link is running a lower software version with FRP enabled.

Help Thy Neighbor Support

VINES services for the router supports the Help Thy Neighbor feature. If a neighbor advertises that a network is unreachable, and the router has an alternative connection to that network, the router issues a "changes only" routing update. This advertises the connection to the neighbor and in the next scheduled update.

For details about the Help Thy Neighbor feature, refer to *VINES Protocol Definition*, Banyan Systems Inc., June 1993.

Using Multipath with Load Sharing

A router on a VINES network does not record multiple nonequal-cost paths to the same destination. However, when one path fails, the router quickly learns these other paths and uses one as an alternate path.

When there are multiple equal-cost paths to a destination network on a VINES network, the router records all of the paths in the VINES routing table. For data transfer to this destination, the router accesses the multiple paths in a round-robin fashion to achieve load sharing.

Partially Meshed Frame Relay Network Support

Some Frame Relay networks are not fully meshed, meaning that some nodes do not have virtual circuits to all other nodes in the network. In that case, to successfully route VINES Security, Net Time, File Service, and StreetTalk packets over the network, the router may have to send frames back through their interface of origin.

Banyan developed Split Horizon so that a router running VINES does not advertise routes to an interface where it learned those routes. However, Split Horizon alone is not sufficient to work on Frame Relay configurations that are not fully meshed. Therefore, you must disable the Split Horizon for STALK Enable parameter. (Refer to "Editing VINES Interface Parameters" in Chapter 4 for details about disabling this parameter.)

For example, if you configure a router in group mode for Frame Relay, Frame Relay treats a group mode circuit like one circuit, even though there are physically two links. If you leave the Split Horizon for STALK Enable parameter set to its default, Enable, the router does not send the VINES packets out through their original interfaces. For VINES to operate successfully, you must disable the Split Horizon for STALK Enable parameter.

Avoiding Address Numbering Problems in LNs and CNs

The default VINES addresses on multi-slot ACE platforms (LNs and CNs) differ in Bay Networks router software version 8.11 and later from previous versions of the router software. The difference is in the way that VINES network addresses are formed on these platforms.

This change in default addresses causes no problems with the routing and operation of any VINES traffic. However, if you use any third-party network management/monitoring software, there may be some problems with VINES address numbering.

To avoid any problems with address numbering, do the following:

1. **Before upgrading the router, obtain the current VINES network address. Use one of the following methods:**

   - From the Technician Interface, enter the following command:

     get wfVinesBase.5.0

   - From the Statistics Manager's Quick Get menu, select wfApplications > wfVinesGroup > wfVinesBaseRouterNetid

     Here is some sample output:

     ```
     wfVinesBase.wfVinesBaseRouterNetid.0=809501872
     ```

2. **Subtract the Banyan assigned base address for Bay Networks (that is, 809500672) from the current address. For example:**

   809501872 - 809500672 = 1200

3. **Set the User-Defined Network ID to equal the result of the previous step. Use one of the following methods:**

   - From the Technician Interface, execute the following command

     set wfVinesBase.4.0 1200;commit

   - From the Configuration Manager, select Protocols > VINES > Global

Note: If you perform Step 3 from the Technician Interface, be sure to save your *config* file before upgrading and rebooting the router.

If you do *not* perform this workaround, routers on the existing VINES network see both old *and* new addresses for 6 minutes (the time it takes for the old number to age out of the router table).

Chapter 3
Enabling VINES Services

This chapter describes how to enable VINES services. It assumes you have read *Configuring and Managing Routers with Site Manager* and that you have

1. Opened a configuration file
2. Specified router hardware if this is a local mode configuration file
3. Selected the link or net module connector on which you are enabling VINES, or configured a WAN circuit if this connector requires one

When you enable VINES services on a circuit, you do not have to configure any VINES parameters. The Configuration Manager supplies default values for all VINES parameters. If you want to edit these default values, refer to Chapter 4.

Enabling VINES on an Interface

To enable VINES on an interface, complete the following steps:

1. **Select VINES from the Select Protocols menu.**

   The Select Protocols menu appears after you either select a link or net module connector, or finish configuring a WAN circuit.

2. **Click on OK to exit from the Select Protocols menu.**

   The window in Figure 3-1 appears.

Figure 3-1. Edit Interface Details Window

3. **Do one of the following:**

   - If you do not want to edit the VINES interface details at this time, click on Cancel.

     If you are enabling VINES on anything *except* a synchronous line, you do not need to take any further steps.

     If you are enabling VINES on a synchronous line, you must specify two synchronous line parameters as described in Step 4.

   - To edit the default values now, click on OK. Refer to Chapter 4 for instructions.

4. **If you are enabling VINES on a synchronous line, you must specify the following:**

   - Clocking source for the synchronous line (internal or external)
   - Synchronous line speed

   To configure these parameters, begin at the Configuration Manager window and proceed as follows:

   a. **Click on the synchronous connector on which you enabled VINES support.**

      The Edit Connector window appears (Figure 3-2).

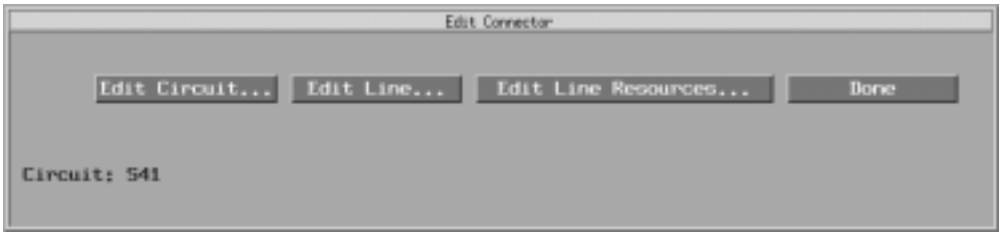

Figure 3-2. Edit Connector Window

b. Click on Edit Line.

The Edit SYNC Parameters window appears (Figure 3-3).

Figure 3-3. Edit SYNC Parameters Window

c. **Set the Clock Source parameter to External or Internal, as appropriate for your network.**

d. **Enter the line speed for the Clock Speed parameter.**

e. **Click on Save to save your changes and exit the window.**

For more information on setting synchronous line parameters, refer to *Configuring WAN Line Services*.

Chapter 4
Editing VINES Parameters

Once you enable a VINES interface, you can use Site Manager to edit VINES parameters and customize VINES services. Site Manager lets you

- Edit VINES global and interface parameters.
- Delete VINES globally from the router.

Note: Before you begin editing, make sure that you configure at least one VINES interface on the router. To configure an interface, or to add more VINES interfaces, refer to Chapter 3 for instructions.

For details on configuring VINES filters, refer to *Configuring Traffic Filters and Protocol Prioritization*.

Accessing VINES Parameters

You access all VINES parameters from the Configuration Manager window (Figure 4-1).

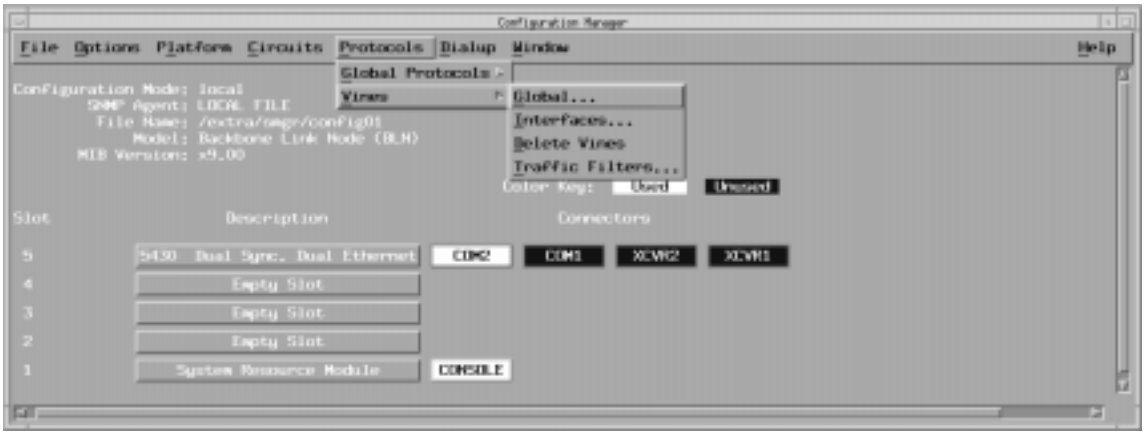

Figure 4-1. Configuration Manager Window

For each VINES parameter, this manual provides information about default settings, valid parameter options, the parameter function, instructions for setting the parameter, and the Management Information Base (MIB) object ID.

The Technician Interface lets you modify parameters by issuing **set** and **commit** commands that specify the MIB object ID. This process is equivalent to modifying parameters using Site Manager. For more information about using the Technician Interface to access the MIB, refer to *Using Technician Interface Software*.

Caution: The Technician Interface does not verify that the value you enter for a parameter is valid. Entering an invalid value can corrupt your configuration.

Editing VINES Global Parameters

To edit VINES global parameters:

1. **Select Protocols > Vines > Edit Vines Global from the Configuration Manager window (Figure 4-1).**

   The Edit VINES Global Parameters window appears (Figure 4-2).

Figure 4-2. Edit VINES Global Parameters Window

2. **Edit the parameters, using the descriptions in the next section as a guide.**
3. **Click on OK to save your changes and exit the window.**

   The Configuration Manager window reappears.

VINES Global Parameter Descriptions

Use these parameter descriptions as a guide when you configure the parameters on the Edit VINES Global Parameters window (refer to Figure 4-2).

Parameter:	**Enable**
Default:	Enable
Options:	Enable | Disable
Function:	Enables or disables VINES services on the entire router.
Instructions:	Set to Disable if you want to disable VINES. Otherwise, accept the default, Enable.
MIB Object ID:	1.3.6.1.4.1.18.3.5.8.1.2

Parameter:	**Network ID**
Default:	0
Range:	0 to 2097151
Function:	Specifies the router's network ID (network number). The network ID is the 32-bit high-order portion of the node's internet address.
Instructions:	The default value, 0, indicates that the router will assign the network ID. We strongly recommend that you accept the default value so that the router assigns the ID. However, if you assign a different network ID, note the following: - All internet addresses assigned to client nodes in this router's network will begin with the Network ID you specify here. - The VINES router will modify the number you enter here so that the first 11 bits reflect the range of Bay Networks assigned numbers. (For example, if you enter 1 as the network ID, the router will precede this number with 0x304.)
MIB Object ID:	1.3.6.1.4.1.18.3.5.8.1.4

Parameter: **Broadcast Class**

Default: All

Options: All | No Charge | Low Cost | LANs | Server All | Server No Charge | Server Low Cost | Server LANs

Function: Specifies, by class, which nodes residing on the router's interfaces should receive broadcast packets generated by this router. This parameter allows you to control the number of extraneous broadcast packets that nodes receive.

For example, the default class, All, specifies that all nodes residing on the router's interfaces should receive broadcast packets. In contrast, the class Low specifies that only those nodes on interfaces to which a low cost is associated should receive broadcast packets. Refer to Table 4-1 for a list of the broadcast classes and their meanings.

Instructions: We recommend accepting the default, All. Each broadcast class setting is shown in Table 4-1.

MIB Object ID: 1.3.6.1.4.1.18.3.5.8.1.6

Table 4-1. Broadcast Class Options

Broadcast Class	Nodes to Receive Packets
All	All reachable nodes on any interface
No Charge	All reachable nodes except those on media that impose a packet charge
Low Cost	All reachable nodes residing on low-cost media (4800 bits/s serial lines, or faster)
LANs	All reachable nodes on high-speed media (LANs)
Server All	All reachable service nodes, regardless of media cost
Server No Charge	All reachable service nodes except those residing on media that impose a packet charge
Server Low Cost	All reachable service nodes residing on low-cost media (4800 bits/s serial lines, or faster)
Server LANs	All reachable service nodes on high-speed media (LANs)

Parameter:	**RTP Mode**
Default:	Automode
Options:	Automode | Nonsequenced | Sequenced
Function:	Specifies whether this router supports Sequenced RTP only (Sequenced), Nonsequenced RTP only (Nonsequenced), or both Sequenced and Nonsequenced RTP (Automode).
Instructions:	Select Sequenced if you want your router to support Sequenced RTP only, or Nonsequenced if you want your router to support Nonsequenced RTP only. Otherwise, accept the default, Automode, to support both Sequenced and Nonsequenced RTP.
MIB Object ID:	1.3.6.1.4.1.18.3.5.8.1.9

Note: When you change the RTP mode of your router, you must isolate the router to allow other routers to age it. Wait at least 6 minutes before you bring the router back onto the network. (Refer to the "VINES Sequenced Routing Update Protocol" section in Chapter 1 for details about the RTP mode.)

Editing VINES Interface Parameters

To edit a VINES interface:

1. **Select Protocols > Vines > Interfaces from the Configuration Manager window (Figure 4-1).**

   The VINES Interfaces window appears (Figure 4-3).

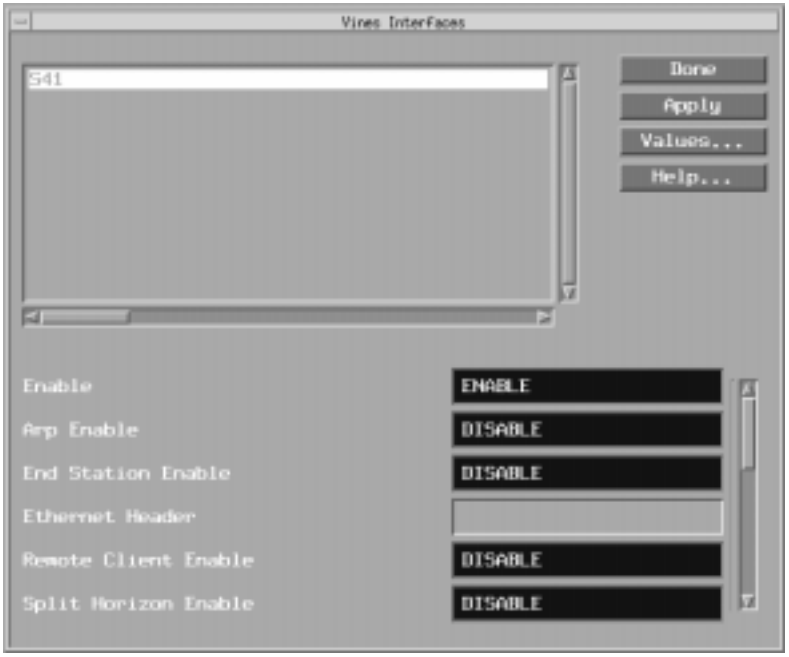

Figure 4-3. VINES Interfaces Window

2. **Edit the parameters, using the descriptions in the next section as a guide.**
3. **Click on Apply to save your changes when you are done.**
4. **Click on Done to exit the window.**

   The Configuration Manager window reappears.

Note: When you reconfigure an interface in dynamic mode, VINES restarts on that interface.

VINES Interfaces Parameter Descriptions

Use these parameter descriptions as a guide to configure the parameters on the VINES Interfaces window (Figure 4-3).

Parameter:	**Enable**
Default:	Enable
Options:	Enable | Disable
Function:	Enables or disables VINES over this interface.
Instructions:	Disable only if you want VINES disabled over this interface. Otherwise, accept the default, Enable.
MIB Object ID:	1.3.6.1.4.1.18.3.5.8.8.1.2

Parameter:	**ARP Enable**
Default:	Disable
Options:	Enable | Disable
Function:	Specifies whether this interface supports VINES ARP. With ARP enabled, the router can provide address resolution services to client nodes on this interface that have not yet been assigned addresses.
Instructions:	Enable ARP only if there are no server nodes on this circuit.
MIB Object ID:	1.3.6.1.4.1.18.3.5.8.8.1.12

Parameter:	**End Station Enable**
Default:	Disable
Options:	Enable | Disable
Function:	Specifies whether this interface supports source routing endstations.
Instructions:	Select Enable if this is a Token Ring interface and if source routing is enabled on the VINES servers and clients in this ring.
MIB Object ID:	1.3.6.1.4.1.18.3.5.8.8.1.13

Parameter:	**Ethernet Header**
Default:	Ethernet
Options:	Ethernet | SNAP
Function:	Specifies the type of encapsulation that this interface supports at the data link level. If this circuit is not an Ethernet circuit, this parameter is ignored.
Instructions:	Accept the default, Ethernet. (Future Banyan VINES releases will support SNAP.)
MIB Object ID:	1.3.6.1.4.1.18.3.5.8.8.1.19

Parameter:	**Remote Client Enable**
Default:	Disable
Options:	Enable | Disable
Function:	When you enable this parameter, client nodes can communicate with server nodes that are multiple hops away by turning off the hop-count decrementor. Also enables serverless WANs.
Instructions:	Enable only if this router also connects to a serverless network segment, and this is the inbound circuit toward the server. Refer to the section "Configuring Routers for Serverless Network Segments" in Chapter 2 for more information.
MIB Object ID:	1.3.6.1.4.1.18.3.5.8.8.1.37

Note: Banyan does not recommend using serverless networks on a WAN because the high cost increases delays and may terminate sessions. We, however, do support such a configuration.

Parameter:	**Split Horizon Enable**
Default:	Disable
Options:	Enable | Disable
Function:	When you enable this parameter, the routes received through an interface are not included in the routing update packets sent out that interface. This parameter is used for debugging purposes only.
Instructions:	Accept the default, Disable.
MIB Object ID:	1.3.6.1.4.1.18.3.5.8.8.1.38

Parameter:	**Interface Cost**
Default:	0
Range:	0 to 65535
Function:	Overrides the default cost specified by Banyan.
Instructions:	To change the default interface cost, you must use the Configured Interface Cost parameter in the VINES Interfaces window.
MIB Object ID:	1.3.6.1.4.1.18.3.5.8.8.1.39

Parameter:	**SMDS Broadcast**
Default:	None
Options:	A multicast address
Function:	Provides a broadcast address for this VINES interface in an SMDS network. If you enter a value for this parameter, then the SMDS switch, rather than the router, will broadcast the message.
Instructions:	Enter the multicast address for all VINES routers provided by the SMDS subscription agreement.
MIB Object ID:	1.3.6.1.4.1.18.3.5.8.8.1.45

Parameter: **Frame Relay Broadcast**

Default: None

Options: Any decimal number

Function: Provides a broadcast address for this VINES interface in a Frame Relay network. If you enter a value for this parameter, then the Frame Relay switch, rather than the router, will broadcast the message.

Instructions: Enter the broadcast address provided by the Frame Relay subscription agreement.

MIB Object ID: 1.3.6.1.4.1.18.3.5.8.8.1.46

Parameter: **Configured MAC Address**

Default: None

Options: The options for this parameter are

- 0
- A user-specified MAC address
- If the interface is on an SMDS circuit, the same complete SMDS E.164 address you entered in the Individual Address parameter box in the SMDS Configuration window

Function: Specifies a MAC (media access control) address for this VINES interface. The router uses its VINES address and this MAC address when transmitting and receiving packets on this interface.

Instructions: Select 0 to configure the router to use its VINES address and the circuit's MAC address when transmitting packets on this interface.

Enter your own MAC address to configure the router to use its VINES address and the specified MAC address when transmitting packets on this interface.

MIB Object ID: 1.3.6.1.4.1.18.3.5.8.8.1.47

Parameter:	**Configured Interface Cost**
Default:	0
Range:	0 to 65535
Function:	Overrides the default Banyan specified cost.
Instructions:	Select 0 to use the default Banyan specified cost. Otherwise, enter a new cost. For example, enter 3 to override the default Banyan cost and set the cost to 3.
MIB Object ID:	1.3.6.1.4.1.18.3.5.8.8.1.49

Parameter:	**Use of FRP Header**
Default:	Enable
Options:	Enable | Disable
Function:	Specifies whether this interface supports a Fragmentation Protocol (FRP) header.
Instructions:	Disable only if you want the FRP header disabled over this interface. If you want to shift from bridging VINES to routing VINES, you must temporarily disable this parameter. Or, you may want to disable this parameter so that your router can interoperate with other routers that do not support the Fragmentation Protocol.
MIB Object ID:	1.3.6.1.4.1.18.3.5.8.8.1.51

Parameter:	**RTP Generation Enable**
Default:	Enable
Options:	Enable | Disable
Function:	This parameter is reserved for future enhancements.
Instructions:	Accept the default.
MIB Object ID:	1.3.6.1.4.1.18.3.5.8.8.1.61

Parameter:	**Inverse ARP Enable**
Default:	Disable
Options:	Enable | Disable
Function:	Specifies whether this interface supports Inverse ARP.
Instructions:	When you enable this parameter, VINES learns the data link connection identifier numbers for a neighbor in a Frame Relay or ATM network. (Refer to Chapter 2 for details on using Inverse ARP for VINES internet address resolution.)
MIB Object ID:	1.3.6.1.4.1.18.3.5.8.8.1.62

Parameter:	**Split Horizon for STALK Enable**
Default:	Enable
Options:	Enable | Disable
Function:	Specifies whether this interface supports Split Horizon for routing StreetTalk (STALK) packets.
Instructions:	When you disable this parameter, the VINES router supports Frame Relay configurations that are not fully meshed for routing VINES Security, Net Time, File Service, and StreetTalk packets. Accept the default, Enable, if you want to enable Split Horizon.
MIB Object ID:	1.3.6.1.4.1.18.3.5.8.8.1.63

Parameter:	**Use Perm. Nonsequenced Neighbors**
Default:	Disable
Options:	Enable | Disable
Function:	When the RTP mode is set to Automode or Sequenced, this parameter specifies whether the VINES interface treats its nonsequenced neighbors as static or permanent entries in the VINES routing table.
Instructions:	Enable only if the RTP mode is set to Automode or Sequenced and you want to prevent the router from timing out nonsequenced neighbors. Sequenced routers age out their nonsequenced neighbors that reside on a WAN every hour. This causes the router to broadcast full RTP updates, which consumes bandwidth.
MIB Object ID:	1.3.6.1.4.1.18.3.5.8.8.1.64

Deleting VINES from the Router

To delete VINES from all router circuits on which it is currently configured:

1. **Select Protocols > Vines > Delete Vines from the Configuration Manager window (Figure 4-1).**

   A window appears that prompts

   ```
   Do you REALLY want to delete Vines?
   ```

2. **Click on OK.**

   Site Manager returns you to the Configuration Manager window. VINES is no longer configured on the router.

If you look at the Configuration Manager window, you will see that the connectors for circuits on which VINES was the only protocol enabled are no longer highlighted. You must reconfigure the circuits for these connectors. (Refer to *Configuring and Managing Routers with Site Manager* for details on configuring the circuits.)

Appendix A
VINES Default Settings

Table A-1 and Table A-2 show the default settings for VINES parameters in Site Manager. Use the Configuration Manager (and Chapter 4, "Editing VINES Parameters") to edit these default settings.

Table A-1. VINES Global Parameters

Parameter	Default
Enable	Enable
Network ID	0 (means router assigns network ID)
Broadcast Class	All
RTP Mode	Automode

Table A-2. VINES Interface Parameters

Parameter	Default
Enable	Enable
ARP Enable	Disable
End Station Enable	Disable
Ethernet Header	Ethernet
Remote Client Enable	Disable
Split Horizon Enable	Disable
Interface Cost	0
SMDS Broadcast	None
Frame Relay Broadcast	None
Configured MAC Address	0
Configured Interface Cost	0
Use of FRP Header	Enable
RTP Generation Enable	Enable
Inverse ARP Enable	Disable
Split Horizon for STALK Enable	Enable
Use Perm. Nonsequenced Neighbors	Disable

Index

A

acronyms, xiii
addressing in VINES, 1-4
ARP Enable interface parameter, 4-8
assigning network ID, 2-2

B

Banyan VINES. *See* VINES
Broadcast Class global parameter, 4-5

C

clients for VINES, 1-1
Configured Interface Cost interface parameter, 4-12
Configured MAC Address interface parameter, 4-11
connectionless services, 1-8
conventions, text, xii

D

data link layer protocols, 1-7
defaults for VINES parameters, A-1
deleting VINES from the router, 4-14

E

educational services, xv
Enable global parameter, 4-4
Enable interface parameter, 4-8
enabling VINES, 3-1
  on a synchronous line, 2-1
End Station Enable interface parameter, 4-8
Ethernet Header interface parameter, 4-9

F

Fragmentation Protocol, 1-3, 1-7
  header, 4-12
    disabling, 2-5 to 2-6
Frame Relay Broadcast interface parameter, 4-11

H

Help Thy Neighbor support, 2-7

I

IEEE support, 1-3, 1-6
Interface Cost interface parameter, 4-10
Internet Control Protocol (ICP), 1-3, 1-16
Internet Protocol (IP), 1-3, 1-8 to 1-10
  VINES IP header for, 1-8, 1-10, 1-16
Inverse Address Resolution Protocol (Inverse ARP), 2-2
Inverse ARP Enable interface parameter, 4-13

M

MAC address
  specifying for VINES interface, 4-11
multiple paths in VINES, 2-8

N

network ID
  assigning to router, 2-2
Network ID global parameter, 4-4
network organization, 1-1

Nonsequenced Address Resolution Protocol (Nonsequenced ARP), 1-3, 1-15
Nonsequenced Routing Update Protocol (Nonsequenced RTP), 1-3, 1-10 to 1-13

O

OSI
support of, 1-2

P

packet
broadcast, 1-9
destined for the router, 1-9
exception notification, 1-16
maximum length of, 1-8
metric notification, 1-17
nonbroadcast, 1-10
nonsequenced routing redirect, 1-13
nonsequenced routing request, 1-13
nonsequenced routing response, 1-13
nonsequenced routing update, 1-12
TimeSync Service broadcast, 1-10
VINES internet, 1-2
parameters
accessing from Site Manager, 4-2
descriptions for. (Italic)See individual entries
global, 4-3 to 4-6
editing, 4-3 to 4-6
interface, 4-8 to 4-14
editing, 4-7 to 4-14
product support, xv
protocol stack, 1-2
publications, Bay Networks, xiv

R

Remote Client Enable interface parameter, 4-9
router
assigning network ID to, 2-2
configuring
for multiple-hop topologies, 2-3
for serverless segments, 2-2
to source route over Token Ring, 2-4
deleting VINES from, 4-14
RTP Mode global parameter, 4-6

S

Sequenced Address Resolution Protocol (Sequenced ARP), 1-3, 1-16
Sequenced Routing Update Protocol (Sequenced RTP), 1-3, 1-14
serverless segment
configuring router for, 2-2
VINES login location restriction for, 2-3
servers on VINES, 1-1
SMDS Broadcast interface parameter, 4-10
Split Horizon, 2-8
Split Horizon Enable interface parameter, 4-10
Split Horizon for STALK Enable interface parameter, 2-8, 4-13
StreetTalk, 1-3, 2-8
support, Bay Networks, xv
synchronous line
enabling VINES on, 2-1

T

table of all known networks, 1-11
table of neighbors, 1-11
technical publications, xiv
technical support, xv
text conventions, xii
TimeSync Service broadcast packet, 1-10

U

Use of FRP Header interface parameter, 4-12
Use of Perm. Non-Sequenced Neighbors interface parameter, 4-14

V

VINES
- addressing
  - network number in, 1-5
  - overview of, 1-4
  - subnetwork number, 1-5
- architecture of, 1-2
- clients for, 1-1
- defaults for, A-1
- deleting from the router, 4-14
- enabling on a circuit, 3-1
- enabling on a synchronous line, 2-1
- enabling on an interface, 4-4
- Fragmentation Protocol on, 1-3
- Frame Relay network support in, 2-8
- Help Thy Neighbor feature of, 2-7
- implementation notes for, 2-1 to 2-7
- internet packets, 1-2
- login location restriction for, 2-3
- making the transition from bridging to routing in, 2-5 to 2-7
- multiple paths in, 2-8
- naming protocol
  - StreetTalk, 1-3
- network organization of, 1-1
- networking protocols in, 1-3
- overview of, 1-1 to 1-17
- packets, 1-2
- protocol stack in, 1-2
- protocols in
  - address resolution for, 1-3
  - data link layer for, 1-7
- routing tables for
  - table of all known networks, 1-11
  - table of neighbors, 1-11
- servers on, 1-1
- Split Horizon in, 2-8
- StreetTalk in, 2-8